Abstract

Most public key cryptosystems have been constructed based on abelian groups. It is possible to a cryptosystem based on non-commutative properties of groups. It propose a new public key cryptosystem built on finite non abelian groups in this paper. It is convertible to a scheme in which the encryption and decryption are much faster than other well-known public key cryptosystems.

References

4. D. Coopersmith, A. M. Odlzyko, R. SchroeppeL Discrete logarithms in GF(p), Algorithmica
5. T. ElGamal, A public key cryptosystem and a signature scheme based on discrete
6. S. Flannery, Cryptography: An investigation of a new algorithm vs. the
7. T. W. Hungerford, Algebra, Springer Verlag
10. R. Lidl, H. Niederreiter, Introduction to finite fields and their application, Cambridge
    203-209.
14. K. Nyberg, R. Rueppel, A new signature scheme based on DSA giving message
15. S.-H. Paeng, J.-W. Han, B. E. Jung, The security of XTR in view of the determinant,
16. S.-H. Paeng, A provably secure public key cryptosystem using finite non abelian groups,
17. A Myasnikov, V Shpilrain, A Ushakov, Noncommutative Cryptography and Complexity
18. T Boaz, Polynomial-time solutions of computational problems in
19. D Grigoriev, I Ponomarenko, Homomorphic Public-Key Cryptosystems Over Groups and
20. AG Myasnikov, V Shpilrain, A Ushakov, Group-Based Cryptography Advanced Courses
21. M Batty, S Braunstein, A Duncan, S Rees, Quantum algorithms in group theory. Cont.
22. LGuL Wang, K Ota, M Dong, Z Cao, Y Yang, public key cryptosystems based on
23. G Baumslag, B Fine, X Xu, Cryptosystems using Linear Groups Appl. based
    187-198.
24. G Baumslag, B Fine, X Xu, A Proposed Public Key Cryptosystem Using the Modular
25. SS Magliveras, DR Stinson, New approaches to designing public key cryptosystem

Index Terms

Computer Science Applied Mathematics
Keywords

Non-Abelian Group, Public key, Encryption, Decryption